Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 7 May 2026

L. Qin
Zhongguancun Laboratory
B. Maddison
Workonline
D. Li
Tsinghua University
I. Lubashev
Akamai

3 November 2025

A Profile for Traffic Origin Authorizations (TOAs)
draft-qin-savnet-toa-00

Abstract

This document defines a standard profile for Traffic Origin Authorizations (TOAs), a Cryptographic Message Syntax (CMS) protected content type for use with the Resource Public Key Infrastructure (RPKI). A TOA is a digitally signed object that provides a means of verifying that an IP address block holder has authorized an Autonomous System (AS) to originate traffic using source IP addresses within the address block.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 8174 [RFC8174].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 7 May 2026.

Table of Contents

1. Introduction

Source Address Validation (SAV) aims to detect and discard data packets that use a spoofed source IP address. The fundamental concept of the current practice is directionality: for data packets using a given source IP address, only those coming from a specific direction are considered legitimate. BCP84 [RFC8704] introduces a more structured direction-based logic, i.e., identifying the incoming directions for traffic of a given source AS and determining the source prefix space that the AS is authorized to use.

To support such validation, a mechanism is needed to allow entities to verify that an AS has been authorized to originate traffic using one or more prefixes as the source IP address. One of the main challenges is that the current infrastructure for validating the right to originate traffic with a given source address has so far been built almost entirely on top of mechanisms designed to validate the right to originate routing information for destination-based routing. In most cases, where the two use cases overlap, this approach works reasonably well. However, when the traffic origin diverges from the route origin, ambiguity and misalignment arise between the intended use case and the mechanisms being applied.

The purpose of a Traffic Origin Authorization (TOA) is to explicitly authorize an AS to originate traffic using a given prefix as a source address, even when that AS is not authorized to originate any BGP routes to that prefix. A TOA provides a clear separation between the authorization to originate routing information and the authorization to originate data traffic.

This distinction is particularly important in scenarios where traffic is unidirectional and there is no need to attract return traffic via route announcements, or where the return traffic is intentionally directed to another location. Examples include Content Delivery Networks (CDNs) using Direct Server Return (DSR) (see [I-D.ietf-savnet-inter-domain-problem-statement]), IP multicast, and traffic sourced with internal-use prefixes.

The TOA makes use of the template for RPKI digitally signed object [RFC6488], which defines a Cryptographic Message Syntax (CMS) wrapper [RFC5652] for a generic validation procedure for RPKI signed objects. Therefore, to complete the specification of the TOA (see Section 4 of [RFC6488]), this document defines:

* The OID that identifies the signed object as being a TOA. (This OID appears within the eContentType in the encapContentInfo object as well as the content-type signed attribute in the signerInfo object.)

* The ASN.1 syntax for the TOA eContent. (This is the payload that specifies the ASes being authorized to originate traffic as well as the prefixes that the ASes may use as the source IP address.) The TOA eContent is ASN.1 encoded using the Distinguished Encoding Rules (DER) [X.690].

* Additional steps required to validate TOAs (in addition to the validation steps specified in [RFC6488]).

The content of a TOA identifies a list of one or more ASes that have been authorized by the IP address block holder to originate traffic and a list of one or more IP address prefixes within the address block that will be used as the source IP address. The IP address block holder can register one or more TOAs to authorize which ASes can originate traffic using specific prefixes within the block as the source IP address. By registering TOAs, IP address block holders can prevent their source IP addresses from being forged by unauthorized ASes, while allowing legitimate but non-announcing ASes to originate traffic. AS operators can leverage TOAs to improve the accuracy and robustness of SAV, thereby enhancing protection against source address spoofing attacks.

2. The TOA Content Type

The content-type for a TOA is defined as id-ct-trafficOriginAuthz and has the numerical value of 1.2.840.113549.1.9.16.1.TBD.

This OID MUST appear within both the eContentType in the encapContentInfo object and the content-type signed attribute in the signerInfo object (see [RFC6488]).

3. The TOA eContent

The content of a TOA identifies a list of one or more ASes that have been authorized by the address block holder to originate traffic and a list of one or more IP address prefixes within the address block that will be used as the source IP address. A TOA is formally defined as:

```
RPKI-TOA-2025
     { iso(1) member-body(2) us(840) rsadsi(113549)
       pkcs(1) pkcs9(9) smime(16) mod(0)
       id-mod-rpkiTOA-2025(TBD) }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS
```

```
  CONTENT-TYPE
  FROM CryptographicMessageSyntax-2010 -- in [RFC6268]
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
      pkcs-9(9) smime(16) modules(0) id-mod-cms-2009(58) } ;

ct-trafficOriginAttestation CONTENT-TYPE ::=
  { TYPE TrafficOriginAttestation
    IDENTIFIED BY id-ct-trafficOriginAuthz }

id-ct-trafficOriginAuthz  OBJECT IDENTIFIER ::=
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) id-smime(16) id-ct(1) trafficOriginAuthz(TBD) }

TrafficOriginAttestation ::= SEQUENCE {
  version [0]   INTEGER DEFAULT 0,
  asSet         ASSet,
  ipaddrBlocks  SEQUENCE (SIZE(1..2)) OF TOAIPAddressFamily }

ASSet ::= SEQUENCE (SIZE(1..10000)) OF ASID
ASID ::= INTEGER (0..4294967295)

TOAIPAddressFamily ::= SEQUENCE {
  addressFamily  ADDRESS-FAMILY.&afi ({AddressFamilySet}),
  addresses      ADDRESS-FAMILY.&Addresses
                                          ({AddressFamilySet}{@addressFamily}) }

ADDRESS-FAMILY ::= CLASS {
  &afi              OCTET STRING (SIZE(2)) UNIQUE,
  &Addresses
  } WITH SYNTAX { AFI &afi ADDRESSES &Addresses }

AddressFamilySet ADDRESS-FAMILY ::=
  { addressFamilyIPv4 | addressFamilyIPv6 }

addressFamilyIPv4 ADDRESS-FAMILY ::=
  { AFI afi-IPv4 ADDRESSES TOAAddressesIPv4 }
addressFamilyIPv6 ADDRESS-FAMILY ::=
  { AFI afi-IPv6 ADDRESSES TOAAddressesIPv6 }

afi-IPv4 OCTET STRING ::= '0001'H
afi-IPv6 OCTET STRING ::= '0002'H

TOAAddressesIPv4 ::= SEQUENCE (SIZE(1..MAX)) OF TOAIPAddress{ub-IPv4}
TOAAddressesIPv6 ::= SEQUENCE (SIZE(1..MAX)) OF TOAIPAddress{ub-IPv6}

ub-IPv4 INTEGER ::= 32
ub-IPv6 INTEGER ::= 128
```

```
TOAIPAddress {INTEGER: ub} ::= BIT STRING (SIZE(0..ub))

END
```

3.1. The version Element

The version number of the TrafficOriginAttestation entry MUST be 0.

3.2. The asSet Element

The asSet element contains a set of AS numbers that are authorized to originate traffic using source IP addresses within the given IP address prefixes.

3.3. The ipaddrBlocks Element

The ipaddrBlocks element encodes the set of IP address prefixes that the specified set of AS numbers is authorized to use as source addresses when originating traffic.

3.3.1. TOAIPAddressFamily

Within the TOAIPAddressFamily structure, the addressFamily element contains the Address Family Identifier (AFI) of an IP address family. Each addressFamily MUST be either 0001 or 0002. There MUST be only one instance of TOAIPAddressFamily per unique AFI in the TOA.

The addresses field contains IP prefixes as a sequence of type TOAIPAddress.

3.3.2. TOAIPAddress

This element is of type BIT STRING and represents a single IP address prefix [RFC3779].

4. TOA Validation

To validate a TOA, the Relying Party (RP) MUST perform all the validation checks specified in [RFC6488] as well as the following additional specific validation steps:

* The IP address delegation extension [RFC3779] is present in the end-entity (EE) certificate (contained within the TOA), and every IP address prefix in the TOA payload is contained within the set of IP addresses specified by the EE certificate’s IP address delegation extension.

* The EE certificate’s IP address delegation extension MUST NOT contain "inherit" elements as described in [RFC3779].

* The Autonomous System identifier delegation extension described in [RFC3779] is not used in TOAs and MUST NOT be present in the EE certificate.

* The TOA content fully conforms with all requirements specified in Sections 2 and 3.

If any of the above checks fail, the TOA MUST be considered invalid and an error SHOULD be logged.

5. Security Considerations

The security considerations of [RFC6481], [RFC6485], [RFC6488], and [RFC9582] also apply to the TOA object.

6. Operational Recommendations

Operators should exercise care when deciding to register a Traffic Origin Authorization (TOA). A TOA is primarily useful in scenarios where the traffic origin AS and the route origin AS differ. In such cases, registering a TOA provides the necessary authorization for traffic origination while avoiding ambiguity between routing and traffic authorization.

Conversely, when the same AS is both authorized to originate routes (via an existing ROA) and to originate traffic from a given prefix, creating an duplicated TOA would add unnecessary storage and transmission overhead in the RPKI system.

Therefore, operators are RECOMMENDED to follow these practices:

* Operators SHOULD NOT register a TOA that is identical to or covered by an existing ROA, unless there are valid operational reasons.

* TOA registrations SHOULD be periodically reviewed and updated to reflect current operational practices.

Another operational consideration concerns situations where a prefix holder has already signed a ROA for an AS and intends to register a TOA that covers multiple ASes and prefixes. For example, suppose a prefix holder has an existing ROA {AS1, Prefix1} and wishes to create a TOA { (AS1, AS2, AS3), (Prefix1, Prefix2, Prefix3) }. In this case, the portion {AS1, Prefix1} is already covered by the ROA and is therefore redundant within the TOA. A straightforward way to avoid

redundancy would be to split the TOA into smaller objects, such as { (AS1), (Prefix2, Prefix3) } and { (AS2, AS3), (Prefix1, Prefix2, Prefix3) }. However, doing so may unnecessarily increase operational complexity and management overhead. Therefore, it is RECOMMENDED to register a single consolidated TOA covering all relevant ASes and prefixes. The existence of an overlapping ROA does not invalidate the TOA but should be understood in its respective scope: the ROA authorizes route origin, while the TOA authorizes traffic origin. This approach maintains clear semantics between routing and traffic authorization while minimizing operational burden.

Following these recommendations minimizes overhead on the RPKI system while ensuring that TOAs are deployed effectively to enhance Source Address Validation (SAV).

7. Enhancing SAV with TOAs

Without TOAs, current SAV mechanisms (e.g., BAR-SAV [I-D.ietf-sidrops-bar-sav]) typically use BGP data, ROAs, or IRR route objects to determine the legitimate source IP address space of a given AS. However, due to the asymmetry between prefixes used as the source IP address and prefixes advertised into the routing system (as mentioned in Section 1), using BGP data, ROAs, and IRR route objects to perform SAV will cause improper blocks (i.e., blocking legitimate data packets).

By registering TOAs, IP address block holders can prevent their source IP addresses from being forged by unauthorized ASes, while allowing legitimate but non-announcing ASes to originate traffic. AS operators can leverage TOAs to improve the accuracy and robustness of SAV, thereby enhancing protection against source address spoofing attacks.

Discussion: When different ASes are authorized for overlapping prefixes (e.g., there are two TOAs { AS1, 1.2.0.0/20 } and { AS2, 1.2.0.0/24 }), does SAV consider both AS1 and AS2 authorized to source traffic from the more specific prefix (1.2.0.0/24), or only AS2? In the current context, both AS1 and AS2 could be interpreted as authorized for the more specific prefix. If the intent is to restrict AS1 from the more specific prefix, the first TOA could be modified to explicitly exclude the more specific prefix.

8. Summary of Discussions

This section is to be removed before publishing as an RFC.

Recent discussions on the SAVNET mailing list have considered whether it would be feasible to create a special ROA for an AS that is not authorized to originate a route to a given prefix, as an alternative to implementing TOA. Doing so would require extending ROAs or overloading their semantics to cover this use case. The TOA authors consulted ASN.1 experts on this approach, who strongly advised against it. Other participants also recommended against overloading ROA semantics. Accordingly, the current consensus among the TOA authors and several SAVNET participants is that defining a dedicated TOA object represents a more appropriate and robust solution.

Some discussions have also proposed creating a conventional ROA for such scenarios, even though the AS is not authorized to originate routes to the given prefix. However, our analysis indicates that registering such a ROA introduces additional risks of forged-origin hijacking: an attacker could impersonate the AS listed in the ROA and announce a BGP route that would be considered RPKI-valid.

Fundamentally, the choice of how to authorize the traffic origin rests with the prefix holder . If the prefix holder wishes ROAs to include only ASes authorized to originate routes to its prefix, there is a clear need to register a TOA to authorize other ASes to source traffic from the prefix. Conversely, if the prefix holder is unconcerned about forged-origin hijacking or other potential risks, they may instead choose to register a conventional ROA.

9. IANA Considerations

9.1. SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)

IANA is requested to allocate the following in the "SMI Security for S/MIME CMS Content Type (1.2.840.113549.1.9.16.1)" registry:

Decimal	Description	Reference
TBD	id-ct-trafficOriginAuthz	draft-qin-savnet-toa

Table 1

9.2. RPKI Signed Objects Registry

Please add an item for the TOA file extension to the RPKI Signed Object registry (https://www.iana.org/assignments/rpki/rpki.xhtml#signed-objects) as follows:

Name	OID	Reference
Traffic Origin Authorization	1.2.840.113549.1.9.16.1.TBD	draft-qin-savnet-toa

Table 2

9.3. File Extension

Please add an item for the TOA file extension to the "RPKI Repository Name Scheme" registry created by [RFC6481] as follows:

Filename Extension	RPKI Object	Reference
.toa	Traffic Origin Authorization	draft-qin-savnet-toa

Table 3

9.4. SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)

IANA is requested to allocate the following in the "SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)" registry:

Decimal	Description	Reference
TBD	id--rpkiTOA-2025	draft-qin-savnet-toa

Table 4

9.5. Media Type Registry

The IANA is requested to register the media type application/rpki-toa in the "Media Type" registry as follows:

Type name: application
Subtype name: rpki-toa
Required parameters: N/A
Optional parameters: N/A
Encoding considerations: binary
Security considerations: Carries an RPKI TOA. This media type contains no active content. See Section 5 of draft-qin-savnet-toa for further information.
Interoperability considerations: None
Published specification: draft-qin-savnet-toa
Applications that use this media type: RPKI operators
Additional information:
  Content: This media type is a signed object, as defined in [RFC6488], which contains a payload of a list of prefixes and an AS identifier as defined in draft-qin-savnet-toa.
  Magic number(s): None
  File extension(s): .toa
  Macintosh file type code(s): None
Person & email address to contact for further information:
  Lancheng Qin <qinlc@mail.zgclab.edu.cn>
Intended usage: COMMON
Restrictions on usage: None
Change controller: IETF

10. Acknowledgements

The authors would like to thank Jeffrey Haas for his valuable contributions in enriching the use cases and clarifying the challenges described in Section 1. Special thanks also go to Job Snijders, who provided expert feedback on the ASN.1 considerations discussed in Section 8.

11. References

11.1. Normative References

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, DOI 10.17487/RFC3779, June 2004, <https://www.rfc-editor.org/info/rfc3779>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC6481] Huston, G., Loomans, R., and G. Michaelson, "A Profile for Resource Certificate Repository Structure", RFC 6481, DOI 10.17487/RFC6481, February 2012, <https://www.rfc-editor.org/info/rfc6481>.

[RFC6485] Huston, G., "The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure (RPKI)", RFC 6485, DOI 10.17487/RFC6485, February 2012, <https://www.rfc-editor.org/info/rfc6485>.

[RFC6488] Lepinski, M., Chi, A., and S. Kent, "Signed Object Template for the Resource Public Key Infrastructure (RPKI)", RFC 6488, DOI 10.17487/RFC6488, February 2012, <https://www.rfc-editor.org/info/rfc6488>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9582] Snijders, J., Maddison, B., Lepinski, M., Kong, D., and S. Kent, "A Profile for Route Origin Authorizations (ROAs)", RFC 9582, DOI 10.17487/RFC9582, May 2024, <https://www.rfc-editor.org/info/rfc9582>.

[X.690] ITU-T, ""Information Technology - ASN.1 encoding rules: pecification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)"", 2021.

11.2. Informative References

[I-D.ietf-savnet-inter-domain-problem-statement] Li, D., Qin, L., Liu, L., Huang, M., and K. Sriram, "Gap Analysis, Problem Statement, and Requirements for Inter-Domain SAV", Work in Progress, Internet-Draft, draft-ietf-savnet-inter-domain-problem-statement-12, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-problem-statement-12>.

[I-D.ietf-sidrops-bar-sav] Sriram, K., Lubashev, I., and D. Montgomery, "Source Address Validation Using BGP UPDATEs, ASPA, and ROA (BAR-SAV)", Work in Progress, Internet-Draft, draft-ietf-sidrops-bar-sav-08, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-bar-sav-08>.

[RFC8704] Sriram, K., Montgomery, D., and J. Haas, "Enhanced Feasible-Path Unicast Reverse Path Forwarding", BCP 84, RFC 8704, DOI 10.17487/RFC8704, February 2020, <https://www.rfc-editor.org/info/rfc8704>.

Authors' Addresses

Lancheng Qin
Zhongguancun Laboratory
Beijing
China
Email: qinlc@mail.zgclab.edu.cn

Ben Maddison
Workonline
Cape Town
South Africa
Email: benm@workonline.africa

Dan Li
Tsinghua University
Beijing
China
Email: tolidan@tsinghua.edu.cn

Igor Lubashev
Akamai
Cambridge,
United States of America
Email: ilubashe@akamai.com